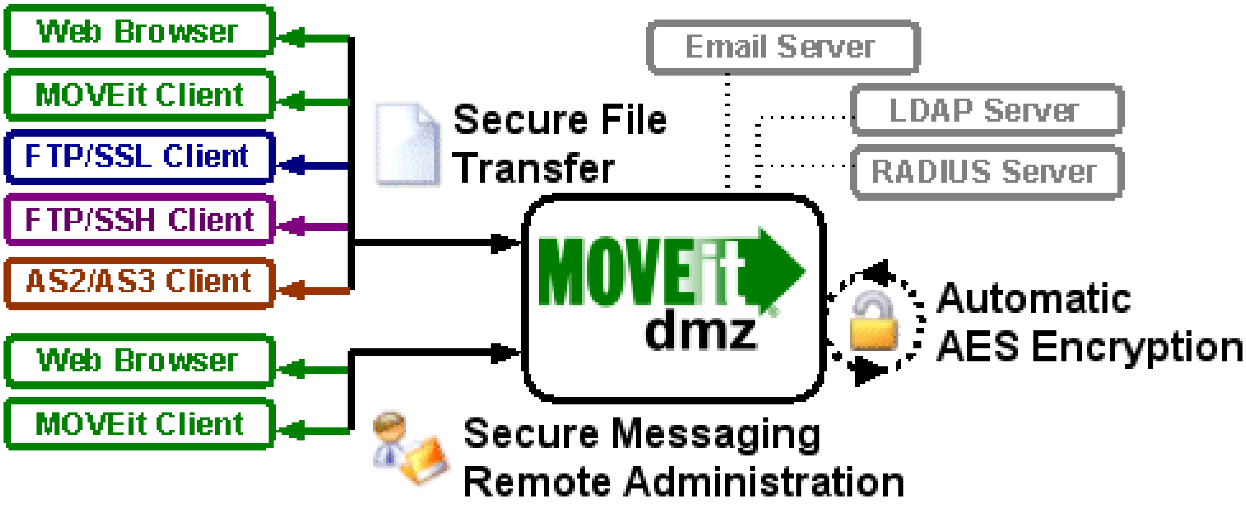
MOVEit® DMZ Manual

v5.5

Contents

Introduction

MOVEit® DMZ is a secure file transfer and secure message server. It is a vital component of the MOVEit® family of secure file processing, storage, and transfer products developed by Ipswitch, Inc.. These products provide comprehensive, integrated, standards-based solutions for secure handling of sensitive information, including financial files, medical records, legal documents, and personal data.



MOVEit DMZ safely and securely collects, stores, manages, and distributes sensitive information between your organization and external entities. Web browsers and no cost/low cost secure FTP clients can quickly, easily, and securely exchange files with MOVEit DMZ over encrypted connections using the HTTP over SSL (https), FTP over SSL (ftps) and FTP over SSH (sftp) protocols. And all files received by MOVEit DMZ are securely stored using FIPS 140-2 validated AES encryption, the U.S. Federal and Canadian government encryption standard.

In addition, a web interface offers easy online administration and monitoring of MOVEit DMZ activities while a programmable interface (via MOVEit DMZ API Windows and MOVEit DMZ API Java) makes MOVEit DMZ accessible to custom applications.

MOVEit DMZ includes an optional MOVEit Wizard plug-in that works with Internet Explorer, Firefox and Mozilla to help web-based users to quickly upload and download large and/or multiple files and folder trees to and from MOVEit DMZ.

Encryption capabilities throughout the MOVEit product line are provided by MOVEit Crypto. The AES encryption in MOVEit Crypto has been FIPS 197 validated. The entire cryptographic module has been FIPS 140-2 validated after rigorous examination by cryptographic specialists in the United States' National Institute of Standards and Technology (NIST) and Canada's Communications Security Establishment (CSE).

FIPS VALIDATED 140-2 ™ MOVEit crypto NIST National Institute of Standards and Technology

Communications Security Establishment Centre de la sécurité des télécommunications Canada

Physical Specifications

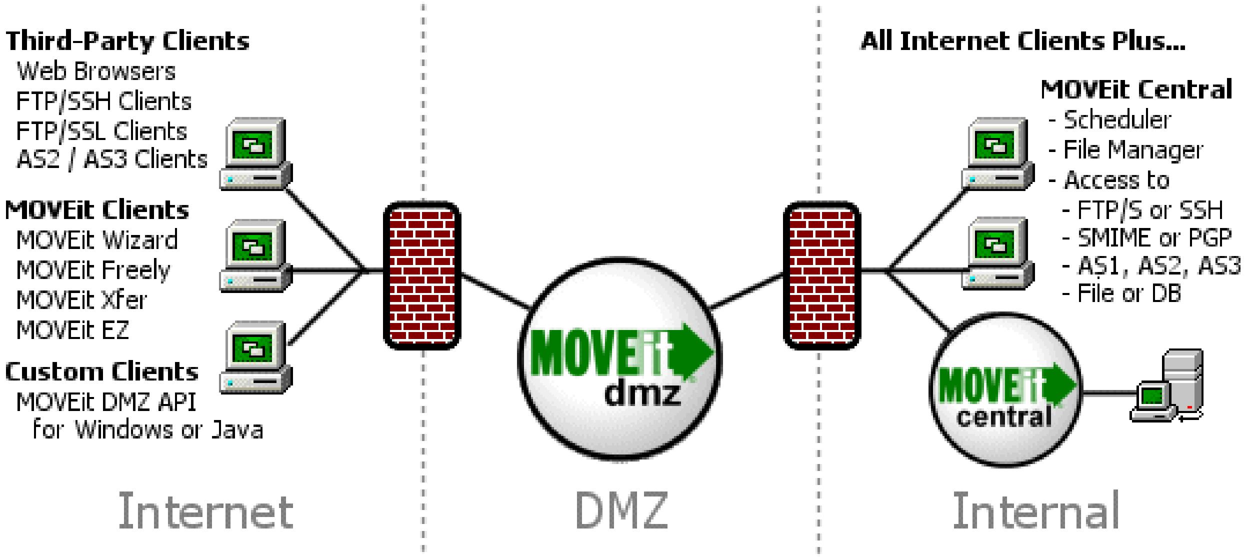
The MOVEit DMZ software itself resides on a Microsoft Windows Server 2003 platform hardened against threats from the Internet and trusted networks. Organizations that need to support very large volumes of file transfers and/or many users may require additional hardware, but for many organizations the minimum recommended specifications of a MOVEit DMZ should suffice:

- 2 GHz Pentium-compatible CPU
- 80 GB SATA or SAS Hard Drive
- 1 GB RAM
- 100/1000 Mb TCP/IP-capable ethernet interface

The latest production recommendations can be found in the online Support Knowledge Base.

Network Specifications

In a typical network topology MOVEit DMZ is best located on a secured "DMZ" segment accessible to both internal and external users."DMZ" is short for DeMilitarized Zone - a network "no man's land" where both internal and internet hosts are allowed to connect. By default connections originating from a DMZ network segment are not to be trusted and are usually not allowed unless there is a compelling case to allow a particular service through.



Web and secure FTP clients can upload and download files to MOVEit DMZ from internal and external networks. For security reasons, MOVEit DMZ is NOT permitted to establish connections with or push files to systems on either your internal network or on an external network. (If a "proxy push" or "proxy store-and-forward" solution is desired, MOVEit Central can be used with MOVEit DMZ to fill this role.)

MOVEit DMZ's Security Advantages Over Other "Secure FTP" Solutions

There are three "areas" where files are at risk when transferred between an external network (such as the Internet) and your internal network:

- When transferred over the INTERNET to a system in your DMZ.
- When temporarily stored on a system in your DMZ.
- When transferred from the system in your DMZ to a system on your internal network.

Most secure Web and FTP file transfer products reside on a system in a DMZ and use industry-standard SSL or SSH to provide secure transfers between the INTERNET and DMZ. (MOVEit DMZ does as well.) Unfortunately, that is as far as most products go; they fail to secure files stored on the DMZ (at risk if the DMZ box gets hacked) and fail to secure files being transfered between DMZ and MY ORG (at risk if a hacker sets up a sniffer inside the DMZ).

MOVEit DMZ secures all three areas by using SSL/SSH-encrypted transfers for ALL transfers and by using FIPS 140-2 validated AES encryption to secure files on disk.

In addition, only MOVEit DMZ offers complete end-to-end file integrity over FTP. In other words, files transferred with secure FTP or web clients which support file integrity checks through the MOVEit system can be proven to be 100% identical to their source files through the use of SHA-1 cryptographic hashes. (When combined with authentication, complete file integrity provides non-repudiation.)

Accessing MOVEit DMZ

"Client" access to MOVEit DMZ is available through several interfaces, including HTTPS, FTP over SSL, and FTP over SSH.

The built-in web interface provides access to anyone with a desktop web browser (i.e. Internet Explorer, Firefox, Netscape, Mozilla, Safari and/or Opera). Authorized administrators may configure the MOVEit DMZ server from authorized locations while customers and partners use a simpler portal to move files in and out of the MOVEit DMZ system.

Also available through the web interface, the optional MOVEit Upload/Download Wizard provides for faster and more reliable file transfers using the web than are normally available through "stock HTTP". The MOVEit Wizard is also the only browser-based client that supports file integrity checking.

A secure FTP interface is also available on the MOVEit DMZ server for people or programs with secure FTP clients. The MOVEit family offers two free, scriptable command-line clients, MOVEit Freely (FTP) and MOVEit Xfer (HTTPS) both of which support file integrity checking. Many third-party companies manufacture secure FTP clients for desktops and servers which will also interface with MOVEit DMZ's secure FTP over SSL and FTP over SSH servers.

For IT departments who desire more control over the MOVEit DMZ environment than the FTP protocol can provide, the MOVEit DMZ API products provide easy access to and control of MOVEit DMZ via a COM object (for Windows) or Java classes (for *nix, Windows, IBM, etc.). MOVEit DMZ API also supports file transfers with full integrity checking and ships with several command-line utilities for administrators who would rather script than program.

If desktop-to-server automation or the ability to access MOVEit DMZ as a local folder is desired, consider using MOVEit EZ. MOVEit EZ is a "tray icon application" which synchronizes content between a user's desktop and MOVEit DMZ and schedules transfers.

When coupled with MOVEit Central and the appropriate licensing, MOVEit DMZ supports AS2 and AS3 file transfer. (MOVEit DMZ can be used as a standalone AS3 server, but without MOVEit Central it has no way of encrypting or decrypting specific messages.)

More information about these clients and the dozens of third-party clients which can also be used to securely exchange files with MOVEit DMZ can be found in the "Client Support" document.

MOVEit Central

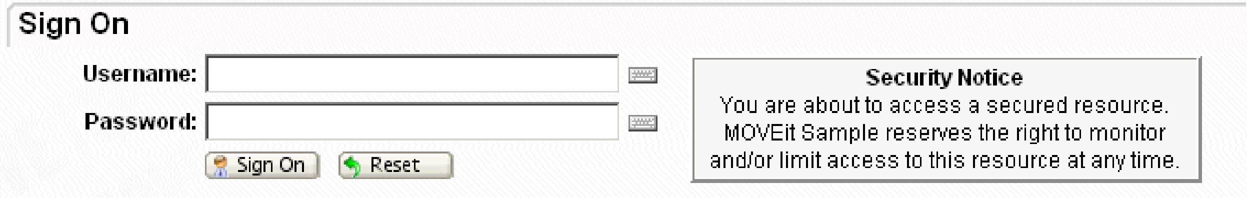
If more than ten scheduled file transfers, immediate movement of files to/from backend servers from MOVEit DMZ, or connectivity to other servers is desired, MOVEit Central is the best tool to use.

MOVEit Central can support thousands of file transfer tasks and is used in production to securely move hundreds of thousands of files a day at major data centers. MOVEit Central instantly knows when a file has arrived on MOVEit DMZ or a Windows file system and can immediately begin transferring that file to its final destination. MOVEit Central supports the most popular secure protocols used across industries, including FTP, SSH, FTP over SSL, SMIME, PGP, email and AS1/AS2/AS3.

In short, when paired with MOVEit DMZ, MOVEit Central completes a secure transfer system which can securely receive, record and send files to/from to almost anyone supporting a secure transfer protocol.

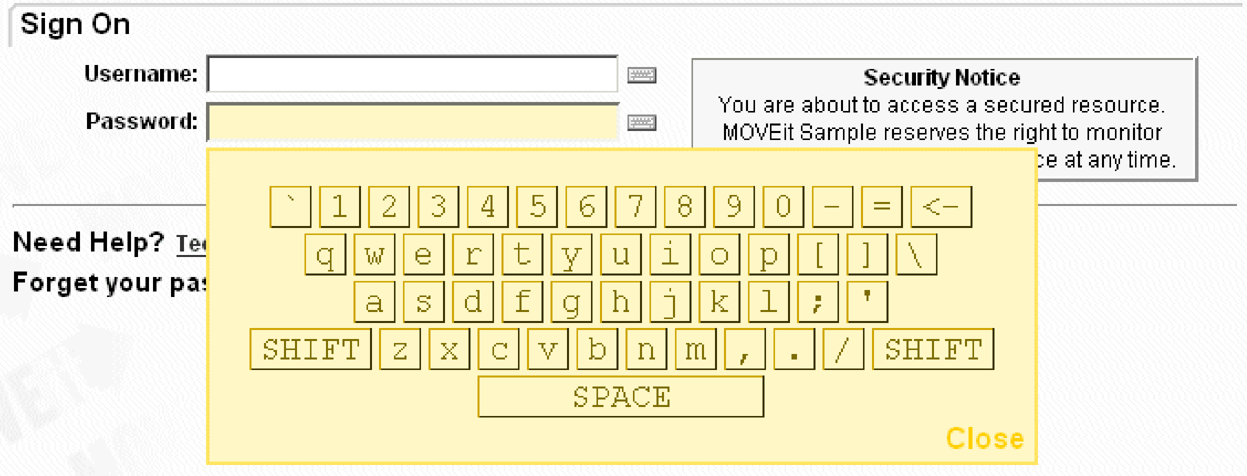
Getting Started - Sign On

The Sign On page is the first page you will see from the MOVEit DMZ site. This page contains fields for a your Username and Password, a "Sign On" button to send this information to MOVEit DMZ and a "Reset" button to clear it.



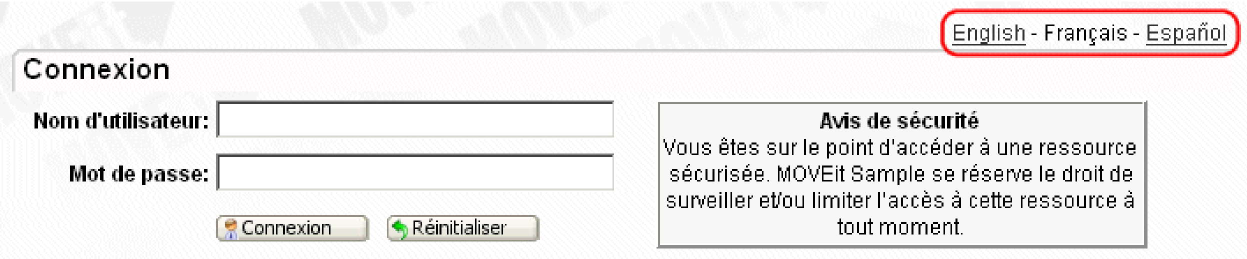
Security Notice
You are about to access a secured resource. MOVEit Sample reserves the right to monitor and/or limit access to this resource at any time.

Clicking on the keyboard icons next to the username and password fields will open a clickable keyboard which can be used to enter your authentication information. Using the clickable keyboard can help thwart keystroke loggers. If you are logging on to the MOVEit DMZ site from a public computer, it is highly recommended you use the clickable keyboard to enter your username and password.



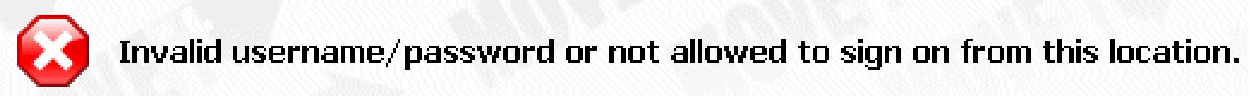
Security Notice
You are about to access a secured resource. MOVEit Sample reserves the right to monitor ce at any time.

If your organization supports multiple languages, MOVEit DMZ will provide links to switch the displayed language. Clicking one of the links will change the Sign On page to display in that language, and set a cookie so your language choice is used the next time you sign on.



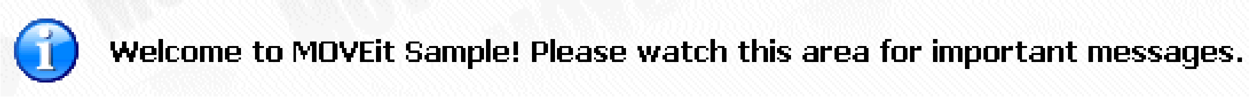
Avis de sécurité
Vous êtes sur le point d'accéder à une ressource sécurisée. MOVEit Sample se réserve le droit de surveiller et/ou limiter l'accès à cette ressource à tout moment.

When you press the Sign On button, your username and password are transmitted securely (via HTTPS) to MOVEit DMZ. If your sign on attempt fails, you will see an error message. If you attempt to sign on too many times in a short period of time you may get locked out of the system altogether. If you need assistance, use the "Tech Support" link on the Sign On page to contact someone you can help you.



Invalid username/password or not allowed to sign on from this location.

If your sign on succeeds you will be rewarded with a success message.



Welcome to MOVEit Sample! Please watch this area for important messages.

The page you will see immediately after signing on depends on how you got to the sign on page in the first place. If you clicked a link from your web browser or typed a short URL into your browser, you are now most likely at the Home Page. If you clicked a link from an email notification, you are now either looking at a secure message or file.

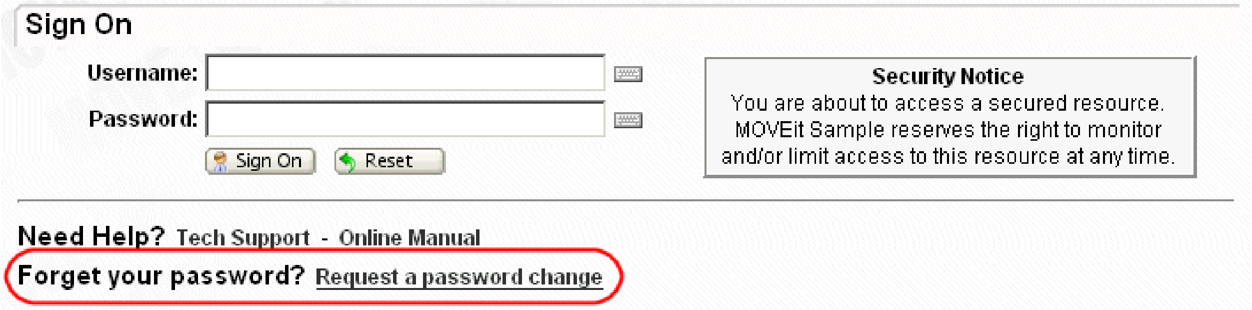
Common Reasons Access is Denied

For security reasons the SAME message is displayed to anyone who fails to sign on for any of the following reasons. (You will only be told that access was denied, not WHY access was denied!)

1. Username is incorrect
2. Password is incorrect
3. Account has been suspended (for too many bad signon attempts, password aging, or manual administrator action)
4. Account is not allowed to sign on from this IP address
5. IP address has been locked out (for too many bad signon attempts, often with different usernames)
6. Client certificate has not been provided when one is required, or a bad client certificate has been provided.

Requesting a Password Change

Some organizations may allow you to request an automatic password change if you have forgotten your password, to avoid a round trip though technical support staff. If this option is enabled, a "Request a password change" link will be present at the bottom of the signon page.



Sign On

Username:

Password:

Security Notice
You are about to access a secured resource.
MOVEit Sample reserves the right to monitor
and/or limit access to this resource at any time.

Need Help? Tech Support - Online Manual

Forget your password? Request a password change

Clicking this link will open the Password Change Request page. This page will prompt you for your username and provide instructions for completing the password change process. Once you enter your username and click the Request Password Change button, an email will be sent to your registered email address, if your account has one, either with instructions for completing the password change, or a notice that the password change was denied.

Client Certificates

Your organization may require you to authenticate to MOVEit DMZ with an SSL (X.509) client certificate ("client cert"). This is common when "two-factor authentication" is required.

All client certs are either "self-signed" or "CA-signed". The "CA-" indicates that a "Certificate Authority" has signed the client cert and vouches for the identity of the bearer. Furthermore, CAs are divided into "commercial CAs" that sell client cert issue and signing services to the general public (e.g., Thawte, GeoTrust, etc.) and "corporate CAs" that perform the same client cert functions for their own users.

MOVEit DMZ supports self-signed certs, commercial CA-signed certs and corporate CA-signed certs, but only your organization can tell you which client certs it will accept for authentication. Your client cert may be delivered to you as a "*.pfx" file with a password or it may be your responsibility to request a client cert from a CA; again only your organization knows the details of this process.

Various browsers have different ways to install client certs. Internet Explorer (IE) uses the Windows Certificate Store; you can either install and manage client certs through IE's "Certificate" dialog (located on the "Content" tab under IE7's "Tools" menu). Windows will also launch a client cert import wizard that will automatically install most client certs into IE if you just double-click "*.pfx" client cert file.

The Mozilla/Firefox line of browsers uses its own client cert store. To install client certs in these browsers you must use their "Certificate Manager". In Mozilla (1.7), this facility is found in the "Privacy & Security" options tree. In Firefox (2.0), this facility is found in the "Encryption" options tab ("View Certificates" button).

Various browsers also have different ways to select client certs for authentication. The most common way is for the browser to simply ask you (via a pop-up dialog) about which client cert to use. When connecting to a MOVEit DMZ server, you may be prompted through your browser to select a client cert after you fill in your username and password or before you view the sign on screen.

However, most browsers also have options to automatically present a client cert if you only have one installed or not ask you about picking a client cert if you did not present one. In these cases you may be using client cert authentication behind the scenes (in the "one cert, so don't ask" case) or not at all (in the "no certs installed, so don't ask" case).

Getting Started - Sign On

Finally, the private key on your client cert may be password protected. If this is the case you may need to type in the password you created when you opted to protect this client cert or key store as well. (Usually, such prompting takes place once per session.)

General Information - Client Support

The following list of clients includes those which have been tested against MOVEit DMZ by Ipswitch and our customers. However, because MOVEit DMZ conforms to HTTP, FTP, SSL and SSH standards, we continue to add to this list as new clients are discovered, developed and/or tested.

In several cases below, the terms "Linux" and "BSD" (two Unix variations) are used interchangeably; please consult the individual vendor's literature for the exact list of platforms supported. Likewise, "Windows" generally covers Microsoft's 32-bit operating systems from Windows 98 through Windows 2003 and Vista, but the exact list of supported operating systems should be obtained from the individual client vendor. (All MOVEit clients have been tested and approved for use under Windows Vista.)

Supported Web Browsers

MOVEit DMZ has been tested against and fully supports the following major browsers:

- Internet Explorer version 5.0 and higher
  - Internet Explorer 5.5 and higher preferred
  - ✓ when using MOVEit Upload/Download Wizard (ActiveX or Java)

- Netscape Navigator version 6.0 and higher
  - Netscape 7.0 and higher preferred
  - ✓ when using MOVEit Upload/Download Wizard (Java - Windows/*nix Only)

- Opera version 6.0 and higher
- Mozilla version 1.0 and higher
  - Mozilla 1.6 and higher preferred
  - ✓ when using MOVEit Upload/Download Wizard (Java - Windows/*nix Only)

- FireFox (all versions)
  - ✓ when using MOVEit Upload/Download Wizard (Java - Windows/*nix/Mac OS X)

- Konqueror under KDE on Linux
- Safari under Macintosh OS X
  - ✓ when using MOVEit Upload/Download Wizard (Java Only)

✓ = Indicates this client can perform integrity checking, an essential requirement of non-repudiation.

At the present time, there are Java bugs in certain browsers which make use of the Java-based MOVEit Wizard impossible in these browsers:

- Opera (all platforms)
- Konqueror (this browser is available only for Linux systems running KDE)
- Mozilla on MacOS (use Firefox instead)

Furthermore, use of the MOVEit Java Wizard on the Macintosh version of Firefox requires that you use the Java Preferences applet to select Java 1.5 (rather than 1.4.2).

As many of the open-source browsers allow end users to "vote" for bug fixes, please contact Ipswitch for information on how to vote for the related bug fixes on your favorite browser. Despite these browser bugs, MOVEit DMZ API for Java, and MOVEit Xfer for Java will still work on these platforms because MOVEit DMZ's core Java transfer code does not depend on the local browser.

Supported Secure FTP/SSL Clients

MOVEit DMZ has been tested against and fully supports a large number of secure FTP clients using FTP over SSL:

- MOVEit Freely ✓ (free command-line)
- MOVEit Buddy ✓ (GUI)
- MOVEit Central ✓ (w/Admin)
- SmartFTP ✓ (GUI, version 1.6 and higher, Windows)
- SmartFTP (free GUI, version 1.0 and higher, Windows)
- WS_FTP Pro (GUI, version 7.0 and higher, Windows)
- Cute FTP Pro (GUI, version 1.0 and higher, Windows)
- BitKinex (GUI, version 2.5 and higher, Windows)
- Glub FTP (GUI, Java 2.0 and higher)
- FlashFXP (GUI, version 3.0 and higher)
- IP*Works SSL (API, Windows, version 5.0)
- LFTP (free command-line, Linux, Unix, Solaris, AIX, etc.)
- NetKit (command-line, Linux, Unix, Solaris, etc.)
- SurgeFTP (command-line, FreeBSD, Linux, Macintosh, Windows, Solaris)
- C-Kermit (command-line; v8.0+, AIX, VMS, Linux, Unix, Solaris)
- AS/400 native FTPS client (OS/400 minicomputer)
- z/OS Secure Sockets FTP client (z/OS mainframe)
- TrailBlaxer ZMOD (OS/400 minicomputer)
- NetFinder (GUI, Apple)
- Sterling Commerce (batch, various)
- Tumbleweed SecureTransport (4.2+ on Windows, batch, various)
- Cleo Lexicom (batch, various)
- bTrade TDAccess (batch, AIX, AS/400, HP-UX, Linux, MVS, Solaris, Windows)
- cURL (command-line, AIX, HP-UX, Linux, QNX, Windows, AmigaOS, BeOS, Solaris, BSD and more)
- South River Technologies "WebDrive" (Windows "drive letter" - requires "passive, implicit and 'PROT P'" options)
- Stairways Software Pty Ltd. "Interarchy" (Mac "local drive" and GUI)

FTP Client Developers: Please consult the "FTP - Interoperability - Integrity Check How-To" documentation for information about how to support integrity checks with your FTP client too.

Supported Secure FTP/SSH (and SCP2) Clients

MOVEit DMZ has been tested against and fully supports the most popular secure FTP clients using FTP over SSH as well:

- OpenSSH sftp for *nix (free command-line, Unix - including Linux and BSD, password and client key modes)
- OpenSSH for Windows (free command-line, Windows, password and client key modes)
- OpenSSH sftp for Mac (preinstalled command-line, Mac, password and client key modes)
- OpenSSH sftp for z/OS (part of "IBM Ported Tools for z/OS", z/OS 1.4+, password and client key modes)
- Putty PSFTP, (command-line, Windows, password and client key modes)
- WS_FTP (GUI, Windows, version 7.0 and higher; version 7.62 has a compression-related bug which prevents it from uploading large, highly compressible files)
- BitKinex (GUI, version 2.5 and higher, Windows)
- F-Secure SSH (command-line, 3.2.0 Client for Unix, password and client key modes)
- FileZilla (GUI, Windows)
- SSH Communications SSH Secure Shell FTP (GUI, Windows, password and client key modes; requires setting # of transfers to 1)
- SSH Tectia Connector (Windows)
- SSH Tectia Client (Windows,AIX,HP-UX,Linux,Solaris)
- J2SSH (free Java class - requires Java 1.3+)
- Net::SFTP - Net::SSH::Perl (free Perl module for Unix)
- MacSSH (GUI, Mac, password mode only)
- Fugu (free GUI, Mac, password mode only)
- Cyberduck (free GUI, Mac, password and client key modes)
- Rbrowser (GUI, Mac, password mode only)
- Transmit2 (GUI, Mac, password and client key modes)
- gftp (GUI, Linux, password and client key modes)
- Magnetk LLC sftpdrive (Windows "drive letter", password mode only)
- South River Technologies "WebDrive" (Windows "drive letter", password mode only)
- Cyclone Commerce Interchange (Solaris, client key mode only)
- Stairways Software Pty Ltd. "Interarchy" (Mac "local drive" and GUI, password mode only)
- Miklos Szeredi's "SSH FileSystem", a.k.a. "SSHFS" (*nix "mount file system" utility, password and client key modes; requires OpenSSH and FUSE)
- Tumbleweed SecureTransport (4.2+ on Windows, batch, various)

Note: Two of the clients above, (OpenSSH for Windows & SSH Communications), are capable of uploading files using multiple independent threads which may send blocks of data non-sequentially. This mode is not supported by MOVEit DMZ SSH and should be disabled using the "-R1" command-line option.

In addition to the SFTP clients listed above, MOVEit DMZ has limited support for some SCP clients. This list of clients is limited to those that implement the SCP2 protocol, which uses SFTP as its underlying transfer mechanism. MOVEit DMZ has been successfully tested with these SCP clients:

- PSCP, (command-line, Windows, password and client key modes)
- F-Secure SCP2 (command-line, 3.2.0 Client for Unix, password and client key modes)
- WinSCP (command-line; SFTP mode)

✓ = Indicates this client can perform integrity checking, an essential requirement of non-repudiation.

MOVEit Central and MOVEit DMZ is the FIRST client and server solution to offer FTP over SSL (ftps) and FTP over SSH (sftp) support in a single product. MOVEit was also the first family of Windows-based products to support all three modes of FTP over SSL transport. Our commitment to full implementation of industry security standards ensures that a wide variety of clients using the FTP protocol over SSL or/and SSH can exchange files with MOVEit DMZ.

Additional FTP over SSL Information:

The three modes of FTP over SSL are:

- TLS-P (aka "Explicit, Always", "SSL" and "TLS")
- TLS-C (aka "Explicit, Negotiate")
- Implicit (usually connected over port 990)

Most administrators prefer their clients to connect to MOVEit DMZ using the IMPLICIT mode of FTP over SSL (TCP port 990). There are two advantages implicit mode enjoys over the other two modes due to its requirement to establish a secure channel before passing any commands at all. (The other two modes connect insecurely on TCP port 21, then build up a secure channel before passing sensitive information.)

- Implicit mode offers fewer interoperability problems because there are almost no options to haggle over during the connection.
- Implicit mode protects against the case where a fumble-fingered user or a poorly written script "leaks" a username, password or other information during the non-secure negotiation of the channel.

Please see the "FTP Server" section of this manual for additional information about supported FTP clients as well as a technical description of secure FTP and what a secure FTP client must do in general to be supported by MOVEit DMZ's secure FTP server.

Supported AS2/AS3 Clients

MOVEit DMZ supports any AS2 client that has been "Drummond" or "eBusinessReady" certified; the software MOVEit DMZ uses to handle incoming AS2 files and MDNs has itself been certified "eBusinessReady" under a program now managed by Drummond.

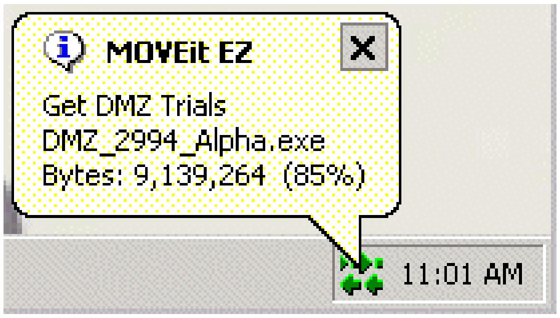
CERTIFIED SOFTWARE
www.ebusinessready.org

AS3 clients are just FTP/SSL clients as far as MOVEit DMZ is concerned. MOVEit Central handles the encryption/decryption, signing and verification of AS files in either case.

User Automation

MOVEit EZ is a Windows desktop client which automatically and securely moves files between MOVEit DMZ and a user's local machine or remote server. End users or applications simply copy files to a designated folder on their local machine and they are whisked away to MOVEit DMZ. Files which are uploaded for that user to MOVEit DMZ are automatically downloaded and placed on their local machine.

MOVEit EZ normally runs as an icon in the tray of an end user, but it is often also installed as a service. During file transfers it will pop open status balloons like the one pictured below to let the end user know it is working. When new files have arrived, the MOVEit EZ icon will change (similar to an email client) to let the end user know something new has arrived.



MOVEit EZ

Get DMZ Trials
DMZ_2994_Alpha.exe
Bytes: 9,139,264 (85%)

11:01 AM

MOVEit EZ supports the concept of guaranteed delivery, which means that it will only accept files which pass a cryptographic integrity check, will resume incomplete transfers and will retry failed transfers.

More information on MOVEit EZ is available on the MOVEit EZ web site. 30-day, self-installing evaluations can be obtained from this page. Site licensing and customized redistribution options (including custom application name and icons) are also available.

Batch File Transfers Involving MOVEit DMZ

Many administrators are utterly addicted to ".bat" scripts for FTP transfers. (.bat files are easy to debug, simple to read and can make use of the built-in ftp.exe client Microsoft ships with every operating system.) Unfortunately, these batch files are limited by ftp.exe itself; specifically, ftp.exe lacks the ability to do passive FTP transfers (often necessary if transferring through firewalls) and secure FTP transfers (recommended for sensitive transmissions over the Internet or other untrusted networks).

MOVEit DMZ (normally) accepts only secure connections, so ftp.exe itself cannot be used to FTP files to and from MOVEit DMZ. However, the MOVEit family provides a FREE and secure alternative for ftp.exe called "MOVEit Freely" (aka "ftps.exe"). If you would prefer to use FTP over SSH transmissions, FREE scriptable clients are available for almost every version of Unix ever invented as well as most Windows operating systems from OpenSSH.

To avoid several all-too-common firewall issues with the FTP/SSL protocol, Ipswitch also offers a FREE HTTPS-based command-line utility called **MOVEit Xfer** that accepts the same syntax and commands as MOVEit Freely and Microsoft's ftp.exe client. Available in both Windows and Java 1.4.2+ versions, this scriptable utility provides single-port secure file transfer on a wide variety of platforms including *nix, Windows, Macintosh and some mainframes.

Copies of MOVEit Xfer and MOVEit Freely are available from the MOVEit support site or from the MOVEit product information site.

Programmatic Control of MOVEit DMZ with MOVEit DMZ API

MOVEit DMZ offers two programming interfaces to Windows and Unix programmers.

MOVEit DMZ API Win(dows)

MOVEit DMZ API is a Windows COM object which allows developers build applications and scripts to exchange secure files and messages with MOVEit DMZ servers, as well as administer folder settings, folder permissions, users and group membership.

MOVEit DMZ API Java (*nix, Windows, Macintosh, Mainframe, etc.)

MOVEit DMZ API Java is a Java class which allows developers build applications and scripts to exchange secure files and messages with MOVEit DMZ servers, as well as administer folder settings, folder permissions, users and group membership.

As these products are separately licensed from MOVEit DMZ, you may contact Ipswitch directly for more information about either of the MOVEit DMZ API products.

Scheduled and Audited File Transfers Involving MOVEit DMZ with MOVEit Central

MOVEit Central is an enterprise file transfer manager capable of simultaneous file transfers to and from hundreds of Windows file systems, FTP/FTPS/SFTP servers, mail servers, web servers, MOVEit DMZ servers and AS1/AS2/AS3 partners.

Includes are a full featured task scheduler, guaranteed delivery, instant (event-driven) transfers, multiple sources/destinations in a single task, the ability to run custom VBScripts against processed files in a fault-tolerant sandbox, and custom event log and/or email notification support. Security features include secure channels for remote control/configuration and AES encryption of configuration information, including remote host credentials.

General Information - Security

The following security features are functions of the MOVEit DMZ software and exist in addition to the hardening of the operating system and associated application services.

Transport Encryption

During transport MOVEit DMZ uses SSL or SSH to encrypt communications. The minimum strength of the encryption used during web transport (e.g., 128-bit") is configurable within the MOVEit DMZ interface.

This value is configurable by organization. To configure this value for any particular organization, sign on as a SysAdmin, view the organization for which this value should be set, and click the "Change Req" link to set the value. NOTE: If you set the minimum encryption value of the "System" organization (#0), you will be given the chance to apply your setting to ALL organizations in the system.

Storage Encryption

MOVEit DMZ stores all files on disk using FIPS 140-2 validated 256-bit AES (http://csrc.nist.gov/encryption/aes), the new (US) federal standard for encryption. MOVEit Crypto, the encryption engine on which MOVEit DMZ relies, is only the tenth product to have been vetted, validated and certified by the United States and Canadian governments for cryptographic fitness under the rigorous FIPS 140-2 guidelines.

MOVEit DMZ also overwrites just-deleted files with random bytes to prevent even encrypted files from lingering on a physical disk after users thought them to have been destroyed.

Precautions Taken During Transport-Storage Exchange

If files received by MOVEit DMZ were simply copied to a large cleartext memory buffer, trojan programs could potentially "sniff" sensitive files out of these spaces.

Instead MOVEitDMZ spools pieces of files received into much smaller buffers, encrypts them and writes them to disk almost immediately. Spooling files in this manner reduces overall exposure in two ways: 1) reduces amount of information exposed and 2) reduces time information is exposed. (This technique also yields some important performance gains.)

(A frequently asked question regarding this issue is "why not just store the file using SSL or SSH" - a short answer to this question is: SSL or SSH uses temporary keys which are renegotiated each time a client establishes a new connection, and we need "more permanent" keys for storage.)

Integrity Checking

When certain file transfer clients are used with a MOVEit DMZ server, the integrity of transfered files will be confirmed. All MOVEit secure FTP, API and web-based clients (including the upload/download Wizard) support integrity checking. Other FTP clients can also take advantage of integrity checks; see "FTP - Interoperability - Integrity Check How-To" for more information.

To perform an integrity check, both the client and the server obtain a cryptographic hash of the transfered file as part of the last step of the transfer. If the values agree, both sides "know" that the file transferred is completely identical to the original. The results of any integrity check are not only displayed to the user of the file transfer client but stored for ready access on the MOVEit DMZ server.

Immediate Transfer off Server

When used with MOVEit Central, MOVEit DMZ supports "event-driven" transfers which allow files to begin spooling to internal servers as soon as they land on an Internet-facing MOVEit DMZ server. This prevents even encrypted files from remaining on the server for longer than absolutely necessary.

Transfer Resume

MOVEit DMZ supports file transfer resume on both its HTTPS and FTPS interfaces. In addition to being useful during transfers of multi-gigabyte file, this feature is also a secure feature in the sense that it makes large file transfers less susceptible to denial-of-service attacks.

Folder Quotas

Enforceable folder size quotas can be set on various folders to prevent system storage from being exhausted.

User Quotas

Enforceable user size quotas can be set on various users to prevent them from exhausting system storage.

Delegation of Authority

Individual end-user members of a group can be designated as Group Admins. These users then are able to administrate the users, folder permissions and address books in their group, subject to various parameters set by organization administrators.

Administrative Alerts

Email notifications are sent to administrators when users are locked out, when the internal consistency checker notices something amiss with the database, etc.

One-Way Workflows

MOVEit DMZ can be configured to never allow users to download what they have just uploaded into the system. This configuration alone can prevent users from misusing MOVEit DMZ as a repository of personal or restricted materials. (Another common way to handle this scenario is through the use of IP restrictions.)

Password Aging

Users can be forced to change their passwords periodically with MOVEit DMZ's password aging features. Users will also be warned (via email) several days in advance of actual expiration, and notified again when their password expires.

Password History

MOVEit DMZ can be configured to remember a certain number of passwords and prevent users from reusing those passwords.

Password Strength Requirements

Various password complexity requirements can be set on MOVEit DMZ, including number/letter, dictionary word and length requirements.

Account Lockout

If someone attempts to sign on to a valid account with an incorrect password too many times, their account can be locked out and administrators will be notified via email.

IP Lockout

A very real concern of administrators of any authenticated resource which supports account lockouts is that someone will get a list of valid usernames and lock all of them out. To mitigate this risk, MOVEit DMZ offers a feature which will prevent a machine with a specific IP address from making any further requests of the system if MOVEit DMZ sees too many bad signon attempts. Administrators will also be notified via email when this occurs.

Restricted IP/Hostname Access

Specific users or classes of users can be restricted to certain ranges of IP addresses and/or hostnames.

Detailed, Tamper-Evident Audit Logging

MOVEit DMZ logs not only signon and signoff events, but permission changes, new user additions and other actions which directly affect the security of the system. Realtime views of this audit trail as well as detailed query tools are available on the Logs and Report pages. All log entries are cryptographically chained together in a way that makes any tampering (add, delete, change) of audit logs evident.

Remote Authentication

MOVEit DMZ's RADIUS and LDAP clients support any standard RADIUS and LDAP servers, including Microsoft's Internet Authentication Server, Novell's BorderManager, Microsoft Active Directory, Novell eDirectory, Sun iPlanet and IBM Tivoli Access Manager (SecureWay).

Obscured Product and Version Identity

MOVEit DMZ does not reveal its product name to unauthorized users via the SSH and FTP interfaces and can be configured to hide this information from web users as well. Version numbers are also only available to authorized users. Obscuring this information prevents hackers from figuring out what they are attacking without doing a fair amount of research.

Client Certificates and Client Keys

All major interfaces of MOVEit DMZ (SFTP, FTPS, HTTPS) support the use of SSL (X.509) client certificates and SSH client keys. SSL client certs and SSH client keys are usually installed on individual machines, but SSL client certificates are also available as hardware tokens.

Multiple Factor Authentication

When used with a username, IP addresses, passwords and client keys/certs offer one-, two- or three-factor authentication.

External Authentication

Organizations worried about storing username-hash combinations on MOVEit DMZ's protected database can use the External Authentication feature and move all non-administrative usernames and passwords to RADIUS or LDAP servers. (Access to the remaining administrative usernames can be locked to specific, internal-only IP addresses.)

Not-In-DMZ Storage Options

There are two ways to store MOVEit DMZ encrypted files in locations that are not in a DMZ. The first is to implement MOVEit DMZ Resiliency and store the data on a remote, logical drive. The second is to deploy MOVEit DMZ on a piece of an existing storage area network (SAN).

Web Browser "Clickable Keyboard" Keystroke Logging Protection

To prevent keystroke logging software and hardware from capturing the keystrokes used to sign on to a MOVEit DMZ using a web browser, a clickable keyboard is provided as an alternate method of data entry. The same keyboard also protects other password fields used throughout the application to protect other users as well.

General Information - Regulations - Privacy/Security/Auditing

This guide answers some questions regarding MOVEit DMZ's expected conformance to HIPAA, FDIC, OCC, G-L-B Act, California SB 1386, Canadian PIPEDA, Payment Card Industry ("PCI"), Sarbanes-Oxley (a.k.a. "SARBOX") and other regulations. Please consult with Ipswitch for the latest information about how MOVEit helps its security-conscious customers achieve their file transfer and storage privacy and security standards as well as relevant contractual, industry and regulatory requirements.

- **"Data at Rest"** - MOVEit DMZ satisfies this requirement by encrypting all files stored on disk with FIPS 140-2 validated 256-bit AES encryption. MOVEit Crypto (the encryption module which powers MOVEit DMZ) is only the tenth product to have been vetted, validated and certified by the United States and Canadian governments for cryptographic fitness under the rigorous FIPS 140-2 guidelines.
- **"Data in Motion"** - MOVEit DMZ satisfies this requirement by using encrypted channels (SSL or SSH) when sending or receiving data.
- **"Tamper-Evident Audit Trail"** - MOVEit DMZ maintains a full audit trail of not only every file transfer but every administrative action as well. All entries are cryptographically chained in a way that makes log tampering (i.e., adding, deleting or changing entries) evident. Scheduled "tamper checks" are run automatically and may also be run manually whenever needed.
- **"Integrity Checking"** - MOVEit DMZ and MOVEit file transfer clients including the Upload/Download Wizard, EZ, Xfer, Freely, Central, API Windows and API Java use cryptographic hashes to verify the integrity of files throughout the transfer chain.
- **"Non-repudiation"** - MOVEit authentication and integrity checking allows people to prove that certain people transmitted and/or received specific files.
- **"Guaranteed Delivery"** - When MOVEit non-repudiation is combined with MOVEit transfer restart and transfer resume features, it satisfies the requirements for a conglomerate concept called "guaranteed delivery".
- **"Obsolete Data Destruction"** - MOVEit DMZ overwrites all deleted files with cryptographic-quality random data to prevent any future access. Specifically, MOVEit DMZ meets the requirements of NIST SP800-88 (data erasure).
- **"Need-To-Know Access Only"** - MOVEit DMZ user/group permissions allow specific access to only those materials users should access.
- **"Good Password Protection"** - MOVEit DMZ requires tough passwords, prevents users from reusing passwords and periodically forces users to change their passwords.
- **"Good Encryption"** - MOVEit DMZ uses SSL to communicate across networks. This "negotiated" protocol can be enforced to connect with 128-bit strength, the maximum currently available. MOVEit DMZ uses MOVEit Crypto's FIPS 140-2 validated 256-bit AES to store data on disk. (This algorithm has been selected by NIST to replace DES, and is faster and more secure than Triple-DES.)
- **"Denial of Service Protection"** - MOVEit DMZ is resilient to DOS attacks caused by resource exhaustion through credential checks or other resources available to anonymous users. ("Nuisance" IP addresses will be locked out.)
- **"Hardening"** - Installation of MOVEit DMZ involves a multi-step (and FULLY documented) hardening procedure which covers the operating system, web service environment, permissions and extraneous applications.
- **"Firewall"** - MOVEit DMZ comes with a detailed firewall configuration guide to minimize confusion on the part of firewall administrators. MOVEit DMZ also supports the use of native IPSec as a

"poor-man's" (packet filtering) firewall as a second line of defense.

- **"Code Escrow"** - The complete source code and build instructions of major (i.e. "3.2") versions of MOVEit DMZ are escrowed with a third-party.
- **"Code Review and Regression Testing"** - All MOVEit DMZ code passes through a code review and change control is maintained with the help of Microsoft's SourceSafe application. Regression testing is performed on each release with an ever-increasing test battery which now includes several thousand tests.
- **"Multiple Factor Authentication"** - When used with a username, IP addresses, passwords and client keys/certs offer one-, two- or three-factor authentication.